AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph on beginning on page 7, line 25 that starts with "WPA further employs" with the following amended paragraph:

WPA further employs a method known ~~know~~ as "Michael" that specifies an algorithm that calculates an 8-byte message integrity code (MIC). The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte integrity check value (ICV). The MIC field is encrypted together with the frame data and the ICV.

Please replace the paragraph on beginning on page 9, line 20 that starts with "If it is unencrypted" with the following amended paragraph:

If it is unencrypted (*e.g.,* type #1), then the user can acknowledge that the network is insecure, and that they wish to use it in spite of that information. However, if it is encrypted and does not use WPA, then it is either of type #2 or #4. If it is type #2, the user would need to enter a WEP key, and if it is type #4, the user does not need to enter a WEP key, but the client computer needs to enable 802.1x authentication to complete the connection. Since the client computer cannot tell whether the network is #2 or #4, it essentially has to ask the user. In the vast majority of cases, the user is in no position (from a technical knowledge perspective) to answer such a question. The introduction of WPS network(s) has made the situation even more complicated (*e.g.,* three different types of encrypted networks).